BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 784 830**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **98 13074**

(51) Int Cl[7] : **H 04 L 9/06**, H 04 L 9/28, G 11 B 23/28, 20/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 19.10.98.

(30) **Priorité** :

(43) **Date de mise à la disposition du public de la demande** : 21.04.00 Bulletin 00/16.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *THOMSON MULTIMEDIA Société anonyme* — FR.

(72) **Inventeur(s)** : FURON TEDDY, CHEVREAU SYLVAIN et DIEHL ERIC.

(73) **Titulaire(s)** :

(74) **Mandataire(s)** : THOMSON MULTIMEDIA.

(54) METHODE DE COPIE EVITANT LA DUPLICATION NON-AUTORISEE DE DONNEES NUMERIQUES ET DISPOSITIF DE LECTURE POUR LA MISE EN OEUVRE DE LA METHODE.

(57) La présente invention concerne une méthode de copie évitant la duplication non-autorisée de données numériques ainsi qu'un dispositif de lecture pour la mise en oeuvre de la méthode.

Selon cette méthode, le support sur lequel doivent être dupliquées les données numériques comporte un numéro de série utilisé pour formater les données numériques lues avant de les écrire sur ledit support.

L'invention s'applique notamment à la duplication des DVD, des CD, des bandes magnétiques ou similaires.

FR 2 784 830 - A1

La présente invention concerne une méthode de copie évitant la duplication non-autorisée de données numériques issues d'une première source sur un support. Elle concerne aussi un dispositif utilisé pour mettre en oeuvre cette méthode.

Les données numériques présentent la propriété de pouvoir être copiées sans perte notable de qualité. En effet, la copie consiste à transmettre de la source vers le dispositif enregistreur une série d'informations binaires, à savoir des « 1 » et « 0 ». Les erreurs survenant habituellement lors de la copie sont facilement corrigées en utilisant des méthodes de correction d'erreurs bien connues. Ainsi, lorsqu'un support d'information ou une source de données contient des données numériques, il est relativement simple de les enregistrer à l'identique sur un support enregistrable.

Pour protéger des données numériques contre la copie illicite, différentes méthodes sont utilisées.

Le plus souvent, le fournisseur munit le support de données numériques tel que la disquette dans le cas d'un logiciel, d'une marque interdisant toute copie.

Une autre façon de protéger des données numériques contre la copie consiste à les doter d'un tatouage ou ''watermark'', c'est-à-dire de données auxiliaires attachées aux données numériques. Le tatouage doit être non-modifiable et non-effaçable. Dans ce cas, la lecture des données se fait à l'aide d'une clé privée qui identifie le tatouage. Lors d'une éventuelle copie des données numériques tatouées, une clé privée est requise pour remettre en place le tatouage sur la copie, sans quoi la copie devient illégale puisque dépourvue de tatouage. Les données numériques copiées sans tatouage ne sont plus lues par le lecteur car celui-ci n'identifie pas de tatouage là où il devrait en trouver un. Ainsi, le tatouage ne permet pas de faire de copie sans la clé privée.

Ces méthodes connues de protection des copies sont en général efficaces lorsque le support est traité par des appareils de lecture ou d'enregistrement conformes. Toutefois, ces méthodes n'évitent pas la

duplication par un pirate qui crée un double ou clone le plus semblable possible à l'original en réalisant ce qui est appelé une copie bit-à-bit.

La présente invention a pour but de proposer une méthode de copie évitant la duplication non-autorisée de données numériques issues d'une première source sur un support ; cette méthode ne permettant pas une copie bit-à-bit des informations numériques.

La présente invention a aussi pour but de fournir un dispositif de lecture comportant des circuits permettant la mise en oeuvre de ladite méthode.

En conséquence, la présente invention a pour objet une méthode de copie évitant la duplication non-autorisée de données numériques issues d'une première source sur un support, caractérisé en ce que le support comporte un numéro de série utilisé pour formater les données numériques lues avant de les écrire sur ledit support.

Selon un mode de réalisation préférentiel, le numéro de série est enregistré de manière infalsifiable sur le support lors de sa fabrication. Pour éviter au maximum tout piratage, le numéro de série est un numéro unique pour chaque support ou présente une faible probabilité d'être commun à deux supports.

D'autre part, le formatage des données numériques à dupliquer est réalisé en utilisant un algorithme de cryptage à clé secrète tel que le D.E.S. ou à clé publique tel que R.S.A., la clé de cryptage étant fonction du numéro de série.

La présente invention concerne aussi une méthode de copie évitant la duplication non-autorisée de données numériques lues par un dispositif de lecture et copiées par un dispositif d'enregistrement sur un support, caractérisé en ce que le support comporte un numéro de série et en ce que la méthode de copie comporte les étapes suivantes :

- envoi du numéro de série enregistré sur le support vers le dispositif de lecture,

- formatage des données numériques lues à l'aide du numéro de série, et

- enregistrement sur ledit support des données numériques formatées.

Selon un mode de réalisation préférentiel, l'étape de formatage est réalisée dans le dispositif de lecture. Ledit dispositif de lecture comporte de plus des moyens permettant de lire le support contenant les données numériques formatées.

Selon une caractéristique supplémentaire de la méthode conforme à la présente invention, avant d'effectuer la duplication des données numériques, la méthode comporte une étape de vérification d'autorisation de copie.

La présente invention concerne aussi un dispositif de lecture comportant un circuit de formatage permettant la mise en oeuvre desdites méthodes de copie décrites ci-dessus.

D'autres caractéristiques et avantages de la présente invention apparaîtront à la lecture de la description d'un mode de réalisation préférentiel faite avec référence au dessin ci-annexé dans lequel :

La figure 1 est une vue schématique sous forme de blocs d'un dispositif de lecture et d'un dispositif enregistreur permettant la copie d'un premier support sur un second support.

La présente invention sera décrite en se référant à la lecture de données numériques enregistrées sur un support numérique tel qu'un DVD pour Digital Video Disc et copiées sur un second support vierge constitué lui aussi par un DVD qui dans ce cas doit être enregistrable, à savoir un DVD-R. Toutefois, il est évident pour l'homme de l'art que d'autres sources d'informations numériques peuvent être utilisées, notamment des informations numériques issues d'un décodeur et envoyées par un "broadcaster" ou des informations numériques stockées sur des supports tels qu'une bande magnétique, un disque optique enregistrable ou non, à savoir un CD, un CD-R, CD-RW, DVD, DVD-R, un disque magnéto-optique ou similaire. Le support d'enregistrement est

constitué par une bande magnétique enregistrable, un CD-R, un CD-RW, un DVD-R ou un disque magnéto-optique permettant de stocker de l'information audio et/ou vidéo sous forme numérique.

Comme représenté sur la figure 1, la méthode de copie conforme à la présente invention permet de copier les informations numériques D enregistrées sur un DVD 1 en utilisant un dispositif de lecture 2 muni d'un circuit de formatage 3 et les données FD qui peuvent être dupliquées, sont enregistrées sur un DVD-R 4 inséré dans un dispositif enregistreur 5.

Conformément à la présente invention, le DVD-R 4 constitué par un DVD-R vierge comporte un numéro de série qui est enregistré de manière infalsifiable lors de la fabrication du DVD-R. Ce numéro de série qui est choisi de manière à être unique ou à présenter une très faible probabilité d'être présent sur deux supports différents, est stocké dans une zone enfouie du disque telle que la zone intitulée « lead-in area » en langue anglaise, à savoir l'amorce de la piste. Comme expliqué de manière plus détaillée ci-après, ce numéro de série est utilisé pour formater les données numériques lues à partir du DVD 1 original.

Conformément à la méthode revendiquée dans la présente invention, les données lues sur le DVD 1 par le dispositif de lecture 2 sont envoyées sur un circuit de formatage 3 qui réalise un formatage des données en utilisant le numéro de série lu sur le DVD-R vierge. On obtient ainsi en sortie du dispositif de lecture des données FD formatées de manière spécifique, qui sont envoyées sur le dispositif enregistreur 5 où elles sont enregistrées sur le DVD-R 4.

Pour réaliser un formatage des données tel que les données enregistrées sur le DVD-R ne puissent pas être copiées bit-à-bit mais puissent toutefois être relues ultérieurement par le dispositif de lecture, à savoir pour réaliser une copie dite licite, différents procédés de formatage peuvent être utilisés. Un des procédés de formatage classique est un algorithme d'encryptage à clé secrète tel que le D.E.S. pour "Date Encryption Standard" en langu anglaise bien connu des spécialistes. Pour éviter toute copie par un pirate, la clé utilisée dans ce cas sera une

clé construite à l'aide d'une clé secrète et du numéro de série lu sur le DVD-R vierge. Pour réaliser l'encryptage en utilisant cet algorithme, les données enregistrées sur le DVD d'origine sont découpées en blocs de 64 bits puis encryptées par le D.E.S. en utilisant une clé de 56 bits obtenue à partir des numéros de série. On obtient en sortie des paquets de données formatées ou chiffrées de 64 bits qui sont enregistrés dans l'appareil d'enregistreur 5 sur le DVD-R 4. Si la clé est constituée par le numéro de série lui-même, le numéro de série comportera 56 bits. Toutefois, le nombre de bits du numéro de série est donné à titre d'exemple. En effet, il est possible d'appliquer l'invention à des supports dont les numéros de série ont des longueurs supérieures ou inférieures à 56 bits. Dans ce cas, on peut appliquer une troncature ou un codage canal pour amener ces numéros de série à la bonne longueur. Si la clé est, pour des raisons de sécurité une fonction du numéro de série, elle peut être obtenue de la manière suivante :

Sachant que NS est le numéro de série du support d'enregistrement, et PS est le paramètre stocké dans les dispositifs de lecture conformes de manière sécurisée :

- on réalise la concaténation de NS et PS pour avoir un mot (NS/PS),
- on applique une fonction de hachage telle que la fonction SHA-1 (standard du National Institute of Standards and Technologies) et l'on obtient comme résultat le mot SHA (NS/PS) ayant une longueur de 64 bits, et
- on réalise une troncature de ce mot pour avoir un mot de 56 bits qui servira de clé pour le DES.

La longueur des mots binaires NS et PS n'est pas fixée, car SHA-1 ne demande pas de longueur précise pour le mot d'entrée. La fonction f s'adapte à toute longueur de numéro de série.

Le DVD-R 4 ainsi copié licitement peut être lu par le dispositif de lecture 2 et les données numériques d'origine sont récupérées en utilisant l'algorithme de décryptage correspondant.

Il est aussi possible de réaliser le formatage des données numériques à dupliquer en utilisant un algorithme à clé publique tel que l'algorithm R.S.A.. Cet algorithme à clé publique est un algorithme asymétrique qui ne permet pas, lorsque l'on connaît la clé publique, de

copier facilement les données formatées lors de leur lecture par le dispositif de lecture 2.

Les données se trouvant sur le DVD-R de copie n'ayant pas la même structure que les données du DVD d'origine, il n'est donc pas possible de les récupérer avec un dispositif de lecture autre qu'un dispositif de lecture conforme. D'autre part, si une copie bit-à-bit du DVD d'origine a été réalisée, le dispositif de lecture de la présente invention ne retrouve pas les informations numériques d'origine et ne va pas la lire.

Selon une caractéristique supplémentaire de la présente invention, la méthode de copie peut être précédée par une étape de vérification d'autorisation de copie telle que celle décrite dans la demande de brevet français n° 98 11860 déposée le 23 septembre 1998 au nom de THOMSON multimédia et ayant pour titre "Protection contre la copie de données numériques stockées sur un support d'information". Cette vérification d'autorisation de copie s'applique à un support d'information comprenant une première identification d'un chiffrage des données numériques, une seconde identification d'un tatouage de données numériques, une première détermination d'une première marque si le chiffrage et le tatouage ont pu être identifiés, une troisième identification d'un type du support d'information, une seconde détermination d'une seconde marque si la première marque a pu être déterminée et si un type déterminé de support d'information a pu être identifié, une quatrième identification de données de signature cryptographique accompagnant les données numériques, une troisième détermination d'une troisième marque si la seconde marque a pu être déterminée et si une donnée de signature cryptographique a pu être identifiée, une première délivrance d'une permission de copie numérique des données numériques si la troisième marque a pu être déterminée.

L'ensemble des caractéristiques décrites dans cette demande de brevet français est incorporé à la présente demande pour réaliser la vérification d'autorisation de copie.

Conformément à la présente invention, le dispositif de lecture 2 des données numériques qui peut être un lecteur de DVD, un décodeur,

un lecteur de CD ou similaire, comporte un circuit de formatage 3 constitué essentiellement par un circuit intégré incluant tous les moyens nécessaires à la réalisation de l'algorithme de cryptage choisi pour le formatage et permettant de stocker de manière infalsifiable certaines données telles qu'une clé secrète ou des moyens d'autorisation de copie.

Le mode de réalisation décrit ci-dessus est donné à titre d'exemple et peut être modifié sans sortir du cadre des revendications ci-jointes.

REVENDICATIONS

1. Méthode de copie évitant la duplication non-autorisée de données numériques issues d'une première source sur un support, caractérisée en ce que le support comporte un numéro de série utilisé pour formater les données numériques lues avant de les écrire sur ledit support.

2. Méthode selon la revendication 1, caractérisée en ce que le numéro de série est enregistré de manière infalsifiable sur le support lors de sa fabrication.

3. Méthode selon l'une des revendications 1 et 2, caractérisée en ce que le numéro de série est un numéro unique pour chaque support ou présente une faible probabilité d'être commun à deux supports.

4. Méthode selon l'une quelconque des revendications 1 à 3, caractérisée en ce que le formatage des données numériques à dupliquer est réalisé en utilisant un algorithme de cryptage à clé secrète tel que le D.E.S. ou à clé publique tel que R.S.A..

5. Méthode selon la revendication 4, caractérisée en ce que la clé de cryptage est fonction du numéro de série.

6. Méthode de copie évitant la duplication non-autorisée de données numériques lues par un dispositif de lecture et copiées par un dispositif d'enregistrement sur un support, caractérisée en ce que le support comporte un numéro de série et en ce que la méthode de copie comporte les étapes suivantes :

- envoi du numéro de série enregistré sur le support vers le dispositif de lecture,
- formatage des données numériques lues à l'aide du numéro de série, et
- enregistrement sur le second support des données numériques formatées.

7. Méthode selon la revendication 6, caractérisée en ce que l'étape de formatage est réalisée dans le dispositif de lecture.

8. Méthode selon l'une quelconque des revendications 6 et 7, caractérisée en ce que le dispositif de lecture comporte des moyens permettant de lire le support contenant les données numériques formatées.

9. Méthode selon l'une quelconque des revendications 4 à 6, caractérisée en ce qu'avant d'effectuer la duplication des données numériques, elle comporte une étape de vérification d'autorisation de copie.

10. Dispositif de lecture comportant un circuit de formatage permettant la mise en oeuvre d'une méthode de copie selon l'une des revendications 1 à 9.

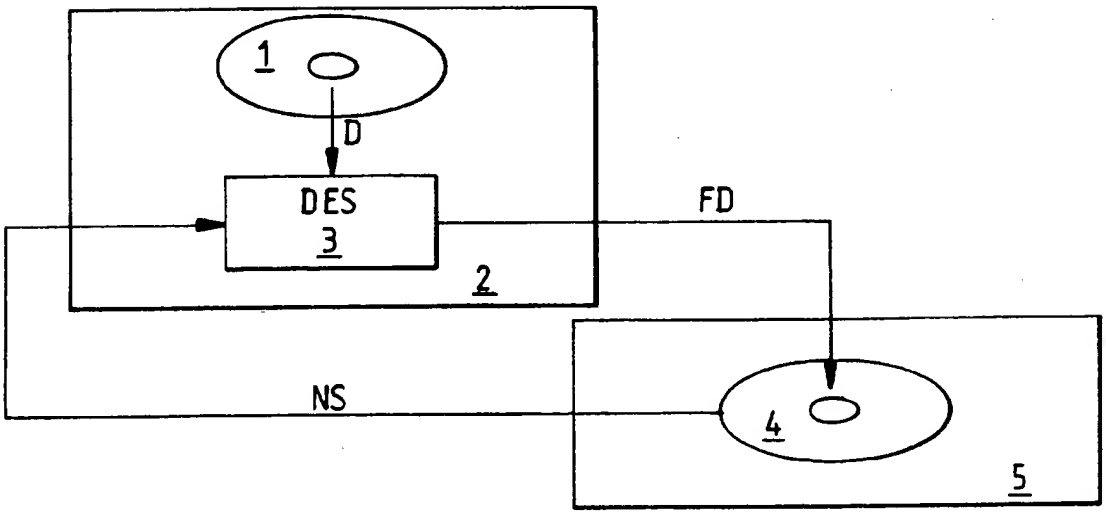

FIG.1

REPUBLIQUE FRANÇAISE

2784830

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 568685
FR 9813074

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée	
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	EP 0 773 490 A (FUJITSU LTD) 14 mai 1997 (1997-05-14) * abrégé * * colonne 1, ligne 44 - colonne 2, ligne 38 * * colonne 3, ligne 48 - colonne 4, ligne 45 * * colonne 5, ligne 30 - colonne 6, ligne 9 * * colonne 9, ligne 46 - colonne 16, ligne 46 * * figures 2,6,12,13 * ---	1-10	
X	PATENT ABSTRACTS OF JAPAN vol. 017, no. 231 (P-1532), 11 mai 1993 (1993-05-11) & JP 04 360068 A (MITSUBISHI ELECTRIC CORP), 14 décembre 1992 (1992-12-14) * abrégé * ---	1-3,6-8, 10	
X	EP 0 785 547 A (IBM) 23 juillet 1997 (1997-07-23) * le document en entier * ---	1-3,6-10	DOMAINES TECHNIQUES RECHERCHES (Int.CL.6) G11B G06F
A	ANONYMOUS: "Preventing Unauthorized Access to Diskette Loaded Microcode. July 1978." IBM TECHNICAL DISCLOSURE BULLETIN, vol. 21, no. 2, pages 836-837, XP002109203 New York, US * le document en entier * --- -/--	1-3,6	

1

Date d'achèvement de la recherche	Examinateur
14 juillet 1999	Schiwy-Rausch, G

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

2784830

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 568685
FR 9813074

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A	EP 0 553 545 A (SEGA ENTERPRISES KK) 4 août 1993 (1993-08-04) * colonne 1, ligne 37 - colonne 2, ligne 12 * * colonne 2, ligne 35 - colonne 3, ligne 20 * * colonne 4, ligne 9 - colonne 5, ligne 26 * * figures 1,2 *	1,2,6
A	EP 0 302 710 A (IBM) 8 février 1989 (1989-02-08) * le document en entier *	1-3,6
A	EP 0 464 320 A (GIGATAPE SYSTEME FUER DATENSIC) 8 janvier 1992 (1992-01-08) * le document en entier *	1-3,6
A	US 5 400 319 A (FITE BARRY A ET AL) 21 mars 1995 (1995-03-21) * figures 4-6 * * colonne 1, ligne 65 - colonne 2, ligne 16 * * colonne 13, ligne 52 - colonne 15, ligne 49 *	1-3
A	ANONYMOUS: "Software Serial Number" IBM TECHNICAL DISCLOSURE BULLETIN, vol. 26, no. 7B, pages 3918-3919, XP002073044 New York, US	
A	EP 0 593 305 A (MATSUSHITA ELECTRIC IND CO LTD) 20 avril 1994 (1994-04-20)	

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

1

Date d'achèvement de la recherche	Examinateur
14 juillet 1999	Schiwy-Rausch, G

EPO FORM 1503 03.82 (P04C13)

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant